

“如何打造下一代公有链”

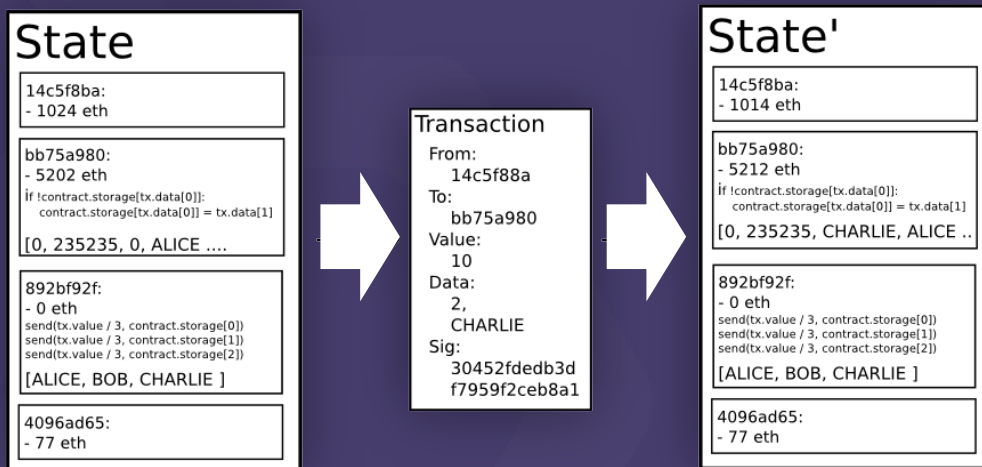
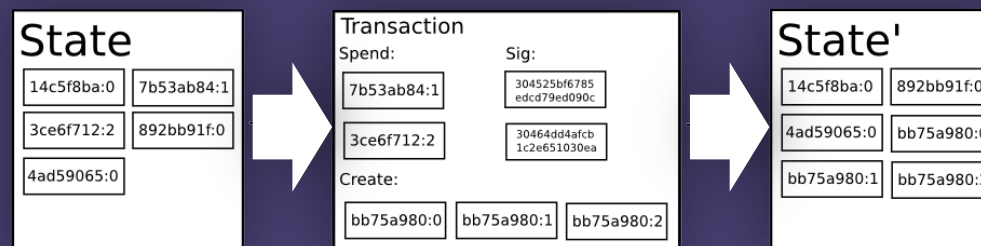


吴为龙

Genaro Network创始人

吉罗科技CTO

Bitcoin State Transition Function



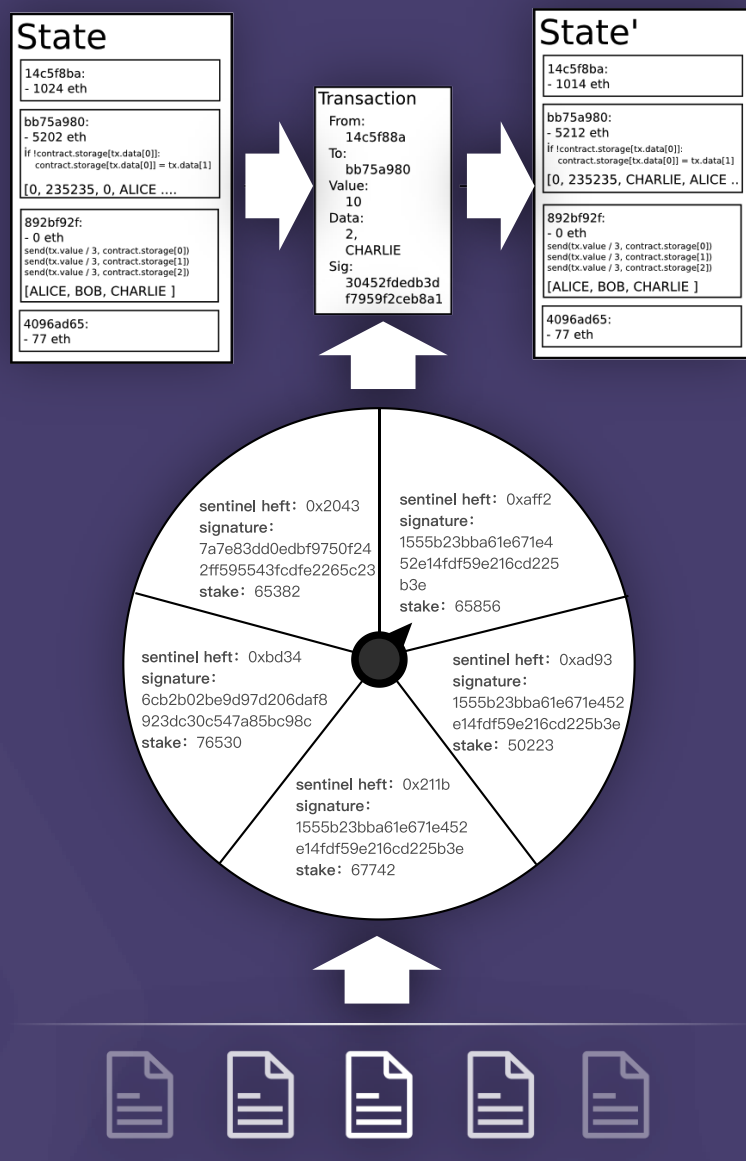
Ethereum State Transition Function





Genaro Network

Genaro 处理方式





- 在PoR系统中，验证方储存的对应加密钥匙。
- 存储文件F会因 为PoR下分割出小的部分，求证方会用这个与文件大小不相关的文件来进行取回
- 加密过程需要将这个sentinel与文件本身相关性低

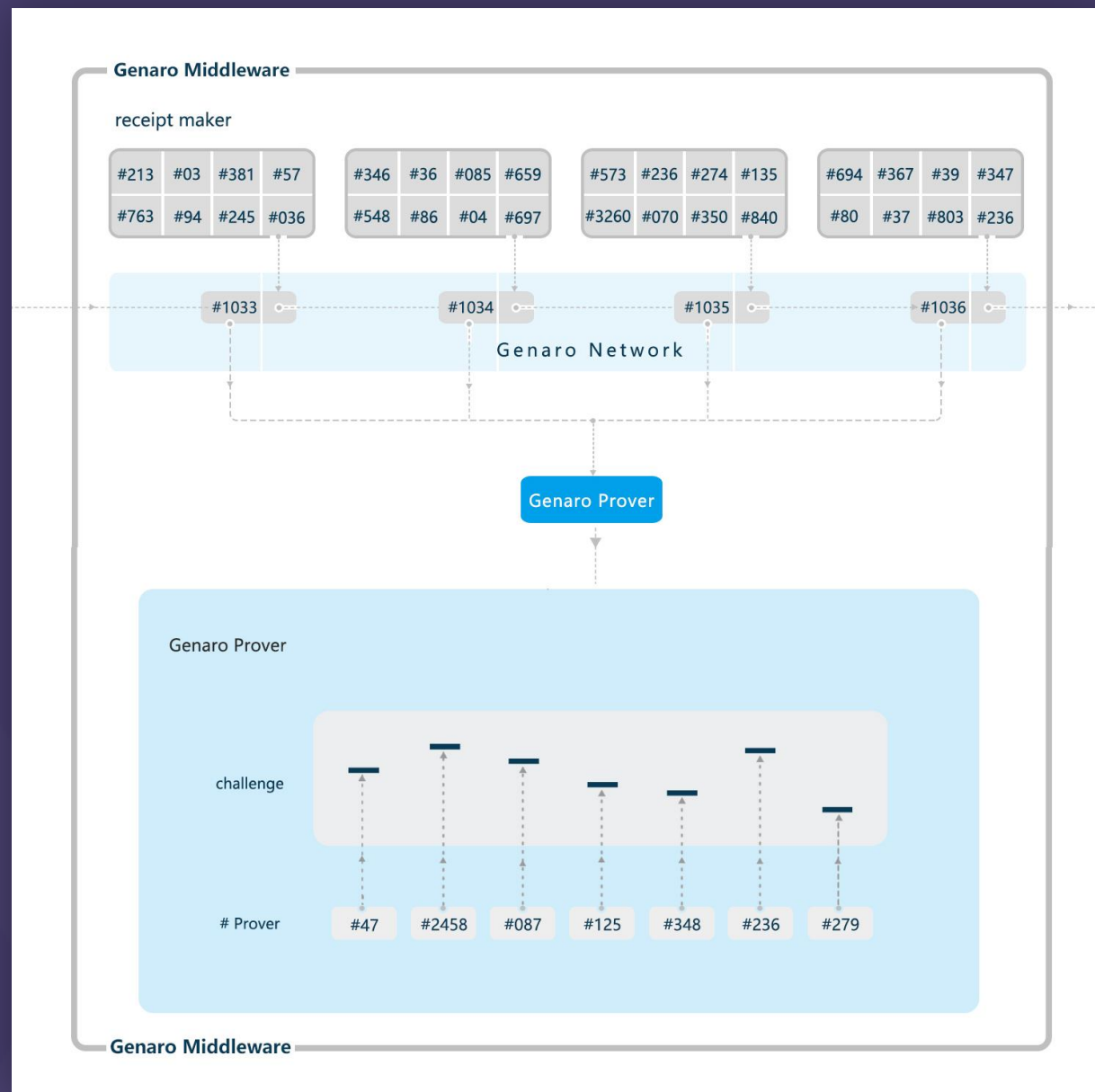




- 能够找回存储的东西 (need a proof)
- 保证其中点对点传输 (need a emule)



Genaro 分布式 存储设计





- 提供proof，作为proof of retrievability中挑战里的重要一环，保证存进网络中的文件可以被取回。
- 在点对点中，很快可以传输，也可以成为共识的辅助。





- 要做共识的补充，我们需要重新定义新的sentinel。
- sentinel要加上类似于开头是0xa0 - 0xb7 来表示对应文件size的 sentinel，作为之后使用。





01. 下一个区块更新的时候，数据库是通过谁来产生的？

02. 下一个区块什么时候产生？

03. 什么交易数据会被放进区块？

04. 怎么解决交易数据历史冲突的问题？





- 在主链使用的共识上，Genaro使用了PoS来获得更低功耗的共识。
- 同时PoS带来的问题，需要使用之前提到的新sentinel来辅助



PoS 解决方案

PeerCoin

使用币龄的概念，开始
使用PoS

DPoS (Delegated PoS)

DPoS 使用投票来解决共识并结合PoS

CTFG (Casper the Friendly Ghost)

保证金方式来解决Proof-of-Stake

CFFG(Casper the Friendly Finality Gadget)

使用epoch，使用链端来解决Proof-of-Stake，混合PoW / PoS机制

Genaro

混合SPoR/PoS机制，在维持低消耗的同时，保证高并发以及存储

Ouroboros PoS

分epoch，分阶段，不同的
phrase来组成一个协议

Tendermint

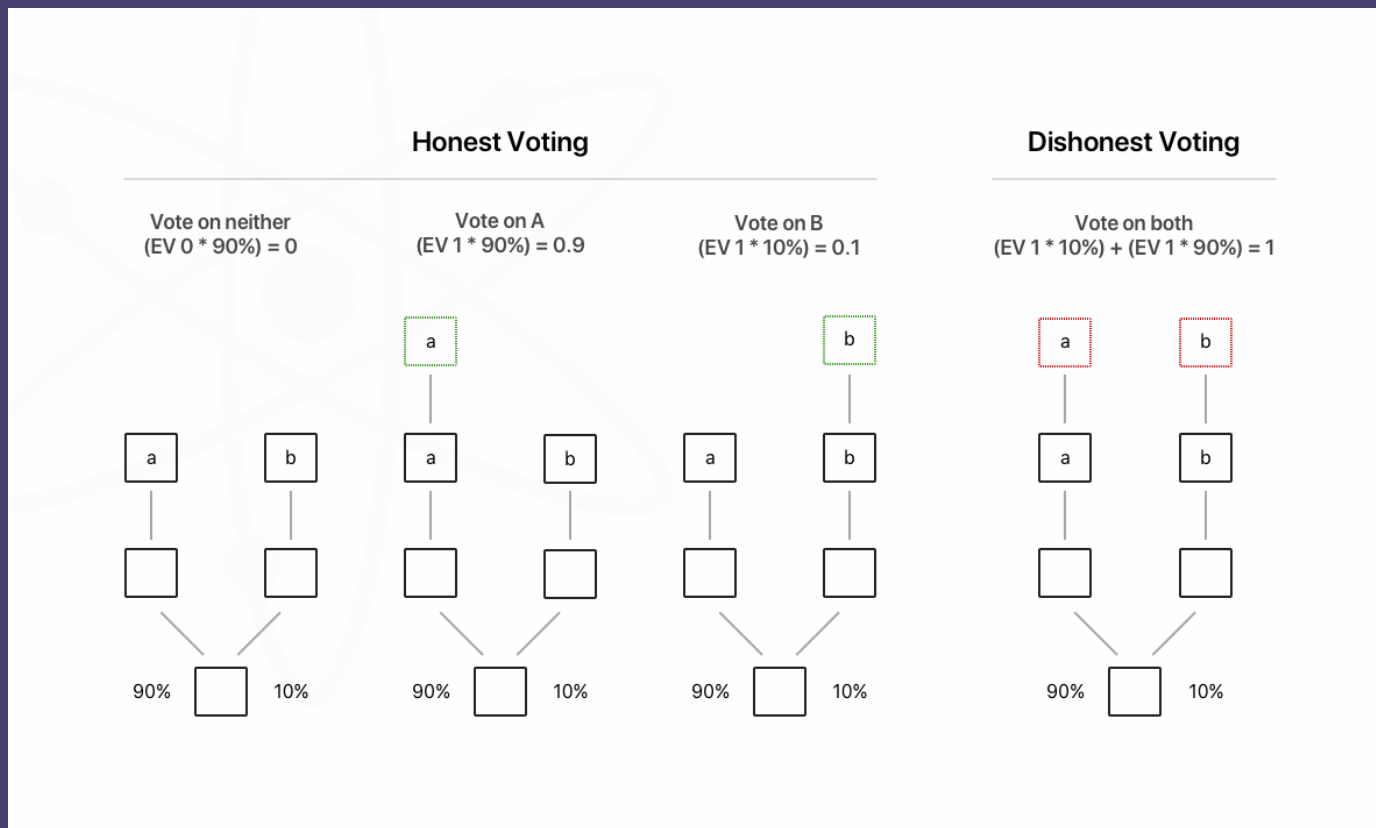
拜占庭方法来解决Proof-of-Stake





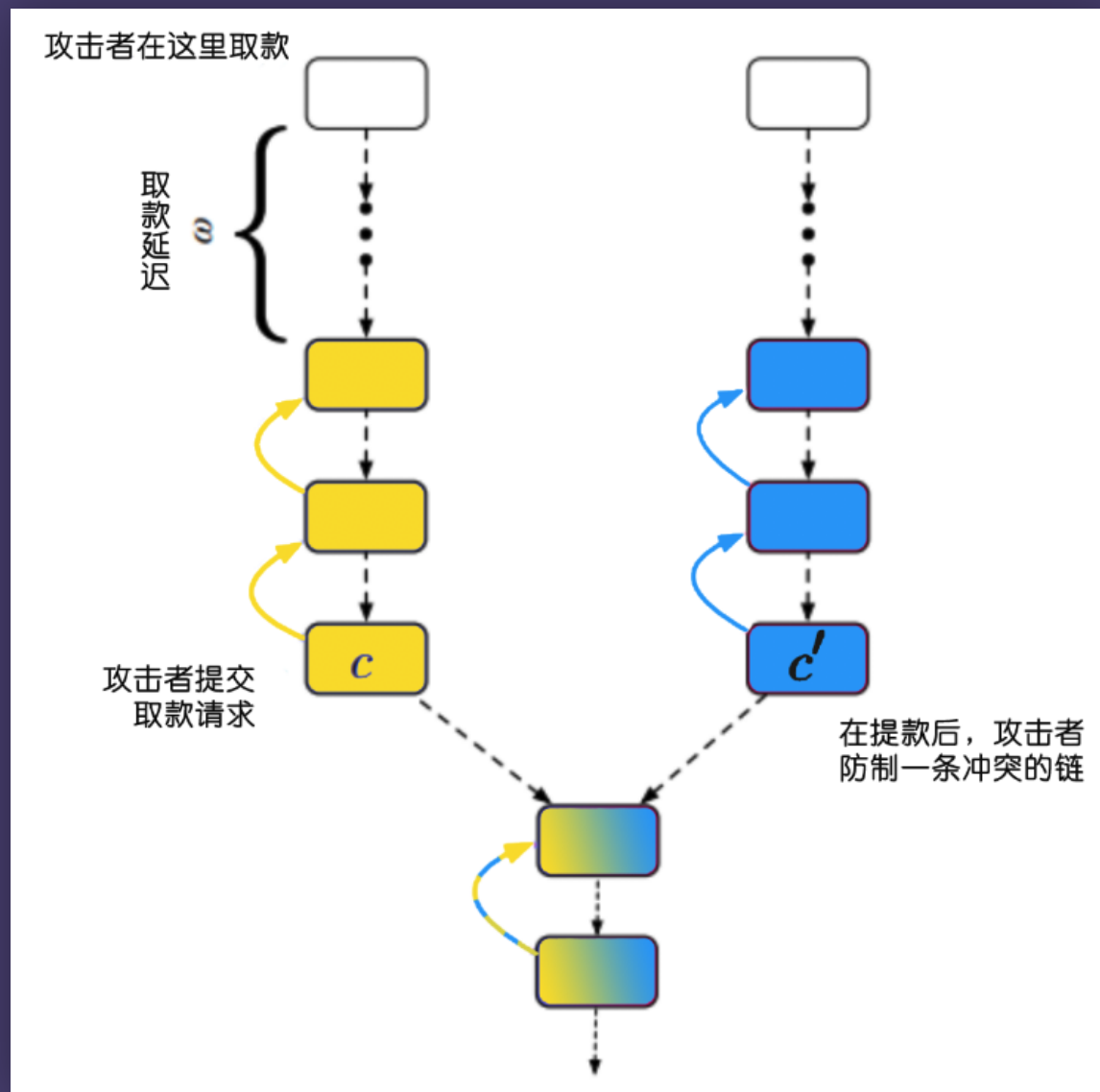
■ 没有承担任何利益

- 如果验证者投给在制定区块高度上不同的几个互相冲突的区块而不受到任何的成成本影响，验证者可以非常高效的破坏共识安全性。





- 一个很基础的问题会由这个而起，因为这个意味着一个攻击者能够制造一个fork从一个非特定的长距离而不会害怕被除去。
- 当2/3的验证者取消绑定之后，他们可以有敌意的创建包含过去验证者的第二个链，然后可以自由的创建另外的交易。





■ 长距离攻击

在解绑利益的时候，同时检查主要的sentinel链条上的检查点，相当于将sentinel heft最高的分支继续演进。

■ 没有承担利益问题

在不同链上不同的权重，拥有主要sentinel的链条上权重比例会高出很多，在非主要链条上，权重为负数。





01. 下一个区块更新的时候，数据库是通过谁来产生的？
挑战者(challenger)
02. 下一个区块什么时候产生？
在混合PoS共识机制结束之后
03. 什么交易数据会被放进区块？
sentinel heft，数据状态，交易状态，Staker的对应签名
04. 怎么解决交易数据历史冲突的问题？
检查sentinel heft 的重量，越重代表是主要的那一条



Genaro Network

Genaro提供混合SPoR/PoS解决方案，
解决可扩展性的同时将储存带入区块链。

Genaro Eden

为每个人提供一个可信任的互联网，通过数据联通现实世界与区块链世界



The collage displays several overlapping screenshots of the Genaro Eden web application interface, which is designed for file storage and wallet management. The interface is clean and modern, with a white background and blue accents.

- File Management Screens:** Several screenshots show the 'My Files' section, displaying a list of files with columns for File Name, Size, Created, and File ID. Files listed include '1 (1).jpg', 'Obc23956699411.59b8fce94a50e.png', '2c084251460959.58ee47e903fe0.png', '01.mp4', and 'Articular_Heavy.otf'. A 'Folders > test' section is also visible.
- Wallet Management Screens:** Other screenshots show the '钱包管理' (Wallet Management) section, displaying account balances and QR codes. For example, 'Account 1' shows a balance of 0.70 and a QR code, while 'Account 2' shows a balance of 0.70 and a QR code. A 'Change Password' button is also visible.
- Account Information Screens:** Some screenshots show the 'Account Information' section, including a 'Restore' button, 'Export The Wallet' button, and a QR code.
- Navigation and Layout:** The interface includes a top navigation bar with the Genaro Eden logo and a sidebar with links to 'My Files', 'Recent', 'Running Task', 'My Wallet', 'Manage Wallet', 'Debits', and 'Share My Storage'.

The overall design is user-friendly and intuitive, with clear labels and easy-to-use buttons. The overlapping nature of the screenshots provides a comprehensive view of the application's features and layout.



Genaro APP

Genaro Eden 的“遥控器” —

Genaro 手机轻钱包 —

“ • In blockchain and storage we trust. ”

• —  Genaro Network

References

- <https://genaro.network/en/documentation/whitepaper>
- <https://github.com/ethereum/wiki/wiki/White-Paper#bitcoin-as-a-state-transition-system>
- <https://easythereentropy.wordpress.com/2014/06/04/understanding-the-ethereum-trie/>
- <https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51>
- http://edcon.io/ppt/one/Vlad%20Zamfir_Casper_EDCON.pdf
- <https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae>
- <https://bitshares.org/technology/delegated-proof-of-stake-consensus/>



关注“UCloud技术公告牌”，更多分享与交流

